Uwaga na ten telefon - fabrycznie zainstalowany szpieg

**Po raz pierwszy w historii specjaliści ds. bezpieczeństwa IT odkryli telefon z fabrycznym oprogramowaniem szpiegującym swojego właściciela.**

Dotychczas wielokrotnie podnoszono kwestie preinstalowanego malware'u na fabrycznie nowych urządzeniach. Słyszeliśmy już o złośliwym oprogramowaniu preinstalowanym na przenośnych pamięciach lub dyskach nowych komputerów, jednak to pracownicy G Data SecurityLabs jako pierwsi na świecie wykryli trojana jako część firmware'u. Ukrywa się on pod wszystkim znaną nazwą Google Play Store i jest jedną ze standardowych aplikacji na badanym telefonie z Androidem. Spyware działa w tle, co skutecznie uniemożliwia jego wykrycie przez właściciela urządzenia. Również bez jego wiedzy smartfon wysyła prywatne dane zapisane w swojej pamięci na serwery znajdujące się w Chinach oraz posiada możliwość instalacji dodatkowych aplikacji.

Opisane funkcje trojana pozwalają na przechwytywanie danych osobowych, połączeń przychodzących oraz informacji wymienianych podczas korzystania z systemów bankowości elektronicznej. Pozwala on także swoim twórcom na zdalne kontrolowanie kamery oraz mikrofonu urządzenia oraz odczytywanie wiadomości e-mail i SMS. Badany model telefonu to N9500 produkowany przez chińską fabrykę STAR i jest łudząco podobny do jednego z flagowców oferowanych przez znanego światowego producenta. Nie ma możliwości usunięcia czy pozbycia się zmanipulowanej aplikacji, tym samym preinstalowanego oprogramowania szpiegującego, gdyż jest ono zintegrowane z oprogramowaniem sprzętowym samego urządzenia (firmware). Sklepy internetowe, także te polskie, posiadają N9500 w swojej ofercie w cenie około 700-800 PLN.

„Funkcje szpiegujące oferowane przez odkryte przez nas złośliwe oprogramowanie są praktycznie nieograniczone. Z ich wykorzystaniem cyberprzestępcy mają pełny dostęp do samego smartfona i zapisanych na nim danych” – mówi Christian Geschkat odpowiadający za produkty mobilne w G Data Software. „To nasi klienci dzięki oprogramowaniu G Data zgłosili wykrycie tej zmasowanej próby kradzieży danych. To pozwoliło nam przyjrzeć się dokładniej taktyce przestępców”.

**Analiza i jej niepokojące wyniki**

Po otrzymaniu informacji od użytkowników, eksperci G Data zamówili urządzenie i rozpoczęli analizę oprogramowania zainstalowanego na telefonie. Pierwszym celem było zidentyfikowanie złośliwego kodu. Firmware zawierał trojana Android.Trojan.Uupay.D ukrywającego się pod aplikacją Google Play Store. Funkcje szpiegujące są całkowicie niewidoczne dla użytkownika i nie można ich w żaden sposób wyłączyć. Co to oznacza w praktyce? Chińscy sprawcy całego zamieszania posiadają całkowity dostęp do urządzenia oraz danych na nim zapisanych. Logi, które mogłyby zdemaskować działanie złośliwego oprogramowania są usuwane, a sam program blokuje instalacje aktualizacji odpowiedzialnych za zapewnienie bezpieczeństwa w systemie z zielonym ludzikiem.

„Jedyną widoczną oznaką działania złośliwej aplikacji jest ikonka sklepu Google w systemowym menedżerze zadań. Niestety, usunięcie trojana nie wchodzi w grę. Jest on częścią oprogramowania sprzętowego telefonu, a aplikacji z tej kategorii nie można odinstalować lub skasować. Tyczy się to także fałszywej aplikacji Google Play na naszym N9500”. Użytkownicy mogą wykryć złośliwe oprogramowanie pod nazwą Android.Trojan.Uupay.D, by przekonać się, czy ich urządzenie zostało dodatkowo wyposażone w oprogramowanie szpiegujące. Jednak, jak radzą eksperci, jedynym logicznym krokiem w tym przypadku jest kontakt ze sklepem i zwrot zakupionego urządzenia.

**Ryzyko dla właścicieli**

Smartfon stanowi poważne zagrożenie dla swoich użytkowników. Złośliwe oprogramowanie pozwala przestępcom na niezauważalną instalację dodatkowych aplikacji, co zwiększa wachlarz ich możliwości: lokalizacja urządzenia i samego użytkownika, przechwytywanie i nagrywanie rozmów, kradzież numerów kart kredytowych wykorzystywanych podczas zakupów online, oszustwa bankowe dzięki przechwytywaniu jednorazowych kodów potwierdzających transakcje czy też wymuszenie na urządzeniu wysyłki kosztownych wiadomości SMS Premium.

Nie ma możliwości dokładnego zlokalizowania serwera, do którego przesyłane są wykradzione dane. „Przechwycone informacje są natychmiast wysyłane do anonimowego serwera w Chinach. Nie jesteśmy w stanie stwierdzić kto jest końcowym adresatem tych informacji” – mówi Geschkat.

**Cena przyciąga!**

Niska cena i przyzwoita specyfikacja urządzenia może być haczykiem przyciągającym klientów. Czterordzeniowy smartfon z 5 calowym wyświetlaczem dostarczany jest z dodatkowymi akcesoriami jak druga bateria i ładowarka samochodowa. Porównując urządzenie do oferty znanych i sprawdzonych producentów, cena N9500 może być nawet 3 krotnie niższa.

Eksperci przypuszczają, że tak niską cenę udało się osiągnąć dzięki zyskom ze sprzedaży nielegalnie pozyskanych danych z zainfekowanych fabrycznie telefonów, które już są w rękach niczego niepodejrzewających użytkowników. „Superokazje i nadzwyczajnie niskie ceny w sklepach internetowych powinny zawsze wzbudzać naszą czujność. W życiu nigdy nie ma nic za darmo!” – stwierdza Geschkat.

Źródło: <http://tech.wp.pl/kat,1031195,title,Uwaga-na-ten-telefon-fabrycznie-zainstalowany-szpieg,wid,16702676,wiadomosc.html?ticaid=114087>